Pending Claims

This listing of claims is a courtesy copy of the pending claims. No amendments have been made in this Reply.

1. (Previously Amended) A method of providing authentication services for applications that are running on a client and requiring access to a network based server, the method comprising:

establishing a network connection further comprising an authentication with the network;

generating, responsive to the authentication, a first dynamic seed locally at the network based server;

generating, responsive to the authentication, a second dynamic seed locally at the client without utilizing the first dynamic seed, wherein the generated second dynamic seed is consistent with the first dynamic seed;

generating a first application key independently at the network based server corresponding to the locally generated first dynamic seed, wherein the first application key is generated without the client intervention;

generating a second application key independently at the client corresponding to the locally generated second dynamic seed, wherein the second application key is generated without utilizing the first application key; and

providing the generated first application key to facilitate authenticating an application at the network based server and the generated second application key to facilitate authenticating an application at the client.

2. (Previously Amended) The method of claim 1 wherein generating the first application key further comprises storing the first application key at the network based server for subsequent retrieval to facilitate the authenticating an application and wherein generating the second application key further comprises storing the second application key at the client for subsequent retrieval to facilitate the authenticating an application.

3. (Previously Amended) The method of claim 1 wherein generating the first application key further comprises generating a plurality of application keys where each of the plurality of keys corresponds to a different application and wherein generating the second application key further comprises generating a plurality of application keys where each of the plurality of keys corresponds to a different application.

4. (Previously Amended) The method of claim 1 wherein providing the first application key further comprises providing an application seed and generating keying information specific to the application and wherein providing the second application key further comprises providing an application seed and generating keying information specific to the application.

5. (Previously Amended) The method of claim 1 wherein providing the first application key further comprises providing a new application key every time the authenticating the application is required and wherein providing the second application key further comprises providing a new application key every time the authenticating the application is required.

6. (Previously Amended) The method of claim 1 wherein providing the first application key further comprises providing the first application key corresponding to a time duration within which the first application key is valid and wherein providing the second application key further comprises providing the second application key corresponding to a time duration within which the second application key is valid.

7. (Previously Amended) The method of claim 1 wherein generating the first dynamic seed further comprises generating a new dynamic seed each time an authentication with the network occurs, the generating the first application key further comprises generating a new application key corresponding to the new dynamic seed, and the providing the first application key further comprises providing the new application key.

8. (Original) The method of claim 1 wherein the authentication with the network utilizes processes corresponding to an Extensible Authentication Protocol.

9. (Original) The method of claim 1 implemented by one of a client and a network server.

10. (Original) The method of claim 9 implemented by one of a wireless client and a network server accessed via a wireless network.

11. (Previously Amended) A computer readable medium storing programming instructions for operating a system entity to provide authentication services for applications that are running on a client and requiring access to a network based server, including programming instructions for:

establishing a network connection and completing an authentication with the network, the authentication generating a first dynamic seed locally at the network based server and generating a second dynamic seed locally at the client, wherein the second dynamic seed is generated without utilizing the first dynamic seed;

generating a first application key independently at the network based server based on the first dynamic seed and a second application key independently at the client based on the second dynamic seed, wherein the first application key is generated without the client intervention; and

providing, on demand, the first and second application keys to facilitate authenticating an application.

12. (Previously Amended) The computer readable medium of claim 11 wherein the programming instructions for storing the first application key in persistent storage at the network based server and the second application key in persistent storage at the client for subsequent retrieval to facilitate the authenticating an application.

13. (Previously Amended) The computer readable medium of claim 11 wherein the programming instructions for generating a plurality of application keys where each of the plurality of keys is derived from the first and second dynamic seeds and corresponds to a different application.

14. (Previously Amended) The computer readable medium of claim 11 wherein the programming instructions providing the application key further provides an application seed; and wherein the computer readable medium further comprises the programming instructions for using the application seed for generating keying information specific to the application.

15. (Previously Amended) The computer readable medium of claim 11 wherein the programming instructions for providing a different application key every time the authenticating the application is required.

16. (Previously Amended) The computer readable medium of claim 11 wherein the programming instructions for providing the first and second application keys and the first and second application keys further corresponds to a time duration within which the application key is valid.

17. (Previously Amended) The computer readable medium of claim 11 wherein the programming instructions for providing a new dynamic seed each time an authentication with the network occurs, and for generating a new application key corresponding to the new dynamic seed and providing the new application key to facilitate the authenticating the application.

18. (Previously Amended) The computer readable medium of claim 11 wherein the programming instructions for completing the authentication with the network utilizes processes corresponding to one of a smart card, an Extensible Authentication Protocol with Subscriber Identity Module extensions, an Extensible Authentication Protocol with Transport Level Security extensions, and an Extensible Authentication Protocol with Authentication and Key Agreement extensions.

19. (Previously Amended) The computer readable medium of claim 11 implemented by one of a client and a network server.

20. (Previously Amended) The computer readable medium of claim 19 implemented by one of a client operating within a wireless communication unit and a network server accessed via a wireless network.